UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/885,234	06/19/2001	Christopher J. Cormack	42390.P11396	4422

			EXAMINER
8791	7590	09/07/2005	LEMMA, SAMSON B

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	**Applicant(s)**
Office Action Summary	09/885,234	CORMACK ET AL.
	Examiner	**Art Unit**	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>24 June 2005</u>.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-30</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1-30</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in replay to an amendment filed on June 24, 2005.

The independent claim 1, 10, 19 have been amended and new claim **28-30**

have been added. **Claims 1-30** are pending.

Response to Arguments

2.   Applicant's argument filed on June 24, 2005 for claims 1-6, 10-15 and 19-24 have been

fully considered but they are not persuasive.

The First argument by the applicant is about the new independent claims 1, 10 and

19, which are amended to includes features which was not part of the former

independent claims. The new features added by the applicant is recited as follows,

"wherein authentication includes at least one chosen from the group consisting

Generating a new user identity value associated with a user identity

and comparing the new user identity value to the stored user identity values and

Obtaining an input responsive to a program attempting to access the

system registry, the input allowing processing to continue." Applicant indicated that

these new features were not disclosed by the reference on the record namely Kathrow.

Examiner disagrees with this argument, examiner would point out that the above

features are disclosed by the former references on the records and the examiner

explanation/remark/argument/citation is included in the respective independent

claims shown below.

The second argument by the applicant is relation to the claims **7-9, 16-18 and 25-**

27, applicant argued that the independent claims 7, 16 and 25 includes features that

was different from the other independent claims 1, 10 and 19 therefore requested a

second consideration with no argument.

Examiner has considered the above request however are moot in view of new

ground(s) of rejection.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form

the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by
another filed in the United States before the invention by the applicant for patent or (2) a patent granted
on an application for patent by another filed in the United States before the invention by the applicant for
patent, except that an international application filed under the treaty defined in section 351(a) shall have
the effects for purposes of this subsection of an application filed in the United States only if the
international application designated the United States and was published under Article 21(2) of such
treaty in the English language.

4.   **Claims 1-6, 10-15,19-24 and 28-30** are rejected under 35 U.S.C. 102(e) as being

anticipated by **Kathrow et al**. (hereinafter referred as **Kathrow**)(U.S. Patent No. 6,263,348)

5.   **As per claims 1-2,10-11 and 28-29** **Kathrow** discloses a method comprising:

●   **Generating a user identity value [hash Value of the user Password]**

associated with a user identity; (In Microsoft operating system, in the process of

authentication, generation of a user identity value or the hash value of the user

password is inherently included. For NT, user enters their password and the clients

hashes the user's password, and generates the hash value or the user identity value

and encrypts the server's challenge with this hash and sends two responses to the

server: One response uses the LAN Manager hash and another response uses the

stronger NT hash. The server then compares the client's response hash with the client's

hash in the SAM Registry hive.)(For the source/explanation that the examiner used, see

reference U, page 2, second paragraph)

- **Storing the user identity value [hash value of the user password]**; (Storing

the **client's hash** or **the user identity value** or **the hash value of the user password**,

in the SAM Registry as explained above for the purpose of authentication is inherently

included in the Microsoft operating system, NT) (For the explanation/source that the

examiner used See reference U, page 2, second paragraph)

Furthermore **Kathrow** discloses

- **Generating a registry security value [Fingerprint of the registry file/s**

  which includes hash value of the Windows registry file/s] associated with a

  system registry; [column 5, lines 11-25; column 4, lines 26-column 5, line 25;

  figure 2, ref. Num "222" and "232"]

- **Storing the registry security value**; [Column 5, lines 11-26; figure 2, ref. Num

  "232"] (content storage stores the fingerprint of the file shown on figure 2, ref.

  Num "232") and

- **Authenticating the system registry after reading the system registry**.(As

  explained in the disclosure and on the dependent claim 5, this limitation

  comprises

- **Generating a new registry security value [Fingerprint of the registry file/s**

  which includes hash value of the Windows registry file/s]; [Column 5, lines

  41-62; figure 2, ref. Num "234"] (The new registry finger print is generated and

  stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security value;**
  [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and **allowing
  processing to continue if the new registry security value is equal to the stored
  registry security value.**[Column 6, lines 32-36; column 10, lines 38-43] (The
  processing will not be allowed to continue if the new registry security value is not equal
  with the stored security value. If this is the case, that is if they are found to be different,
  then the comparison result will be reported.)
  wherein authentication includes at least one chosen from the group consisting of:
  Generating a new user identity value associated with a user identity
  and comparing the new user identity value to the stored user identity values (As
  explained above in Microsoft operating system, in the process of authentication,
  generation of a user identity value or the hash value of the user password is inherently
  included. For NT, user enters their password/could be a new password and the clients
  hashes the user's new password, and generates the hash value or the user identity
  value and encrypts the server's challenge with this hash and sends two responses to the
  server: One response uses the LAN Manager hash and another response uses the
  stronger NT hash. The server then compares the client's response hash with the client's
  hash in the SAM Registry hive and this meets the limitation of generating a new user
  identity value associated with a user identity and comparing the new user identity value
  to the stored user identity values.)(For the source/explanation that the examiner used,
  see reference U, page 2, second paragraph and since the limitation indicated at least
  one choosen from the group consists of the above explanation is sufficient) and
  Obtaining an input responsive to a program attempting to access the
  system registry, the input allowing processing to continue. (Since the limitation
  indicated at least one choosen from the group consists of the above explanation is
  sufficient)

6.   **As per claims 19-20 and 30** **Kathrow** discloses an Apparatus **comprising**:

- **A bus**; [figure 1] (The bus is inherently included in the computer system shown
  on figure 1, it connects the cpu/processor with the memory or storage)

- **Storage device coupled to said bus**;[Figure 1, ref. Num "162" and "164") (The
  storage device shown on figure 1, ref. Num "162 and "164" are coupled to the
  processor by said bus as shown on figure 1) and

- **A processor coupled to said data storage device**, [figure 1, ref. Num "160" and
  "162" and "164")

- **Said processor operable to receive instructions which, when executed by
  the processor, cause the processor to [Column 3, lines 23-27; column 3,
  lines 27-56]**

- **Generating a user identity value [hash Value of the user Password]
  associated with a user identity**; (In Microsoft operating system, in the process of
  authentication, generation of a user identity value or the hash value of the user
  password is inherently included. For NT, user enters their password and the clients
  hashes the user's password, and generates the hash value or user identity value and
  encrypts the server's challenge with this hash and sends two responses to the server:
  One response uses the LAN Manager hash and another response uses the stronger NT
  hash. The server then compares the client's response hash with the client's hash in the
  SAM Registry hive.)(For the explanation/source that the examiner used, see reference
  U, page 2, second paragraph)

- **Storing the user identity value [hash value of the user password]**; (Storing

the **client's hash** or **the user identity value** or **the hash value of the user password**,

in the SAM Registry as explained above for the purpose of authentication is inherently

included in the Microsoft operating system, NT) (For the explanation/source that the

examiner used See reference U, page 2, second paragraph)

Furthermore **Kathrow** discloses

- **Generating a registry security value [Fingerprint of the registry file/s**

  which includes hash value of the Windows registry file/s] associated with a

  system registry; [Column 5, lines 11-25; column 4, lines 26-column 5, line 25;

  figure 2, ref. Num "222", ref. Num "232"]

- **Storing the registry security value**; [Column 5, lines 11-26; figure 2, ref. Num

  "232"] (content storage stores the fingerprint of the file shown on figure 2, ref.

  Num "232") and

- **Authenticating the system registry after reading the system registry.**(As

  explained in the disclosure and on the dependent claim 5, this limitation

  comprises

- **Generating a new registry security value [Fingerprint of the registry file/s**

  which includes hash value of the Windows registry file/s]; [Column 5, lines

  41-62; figure 2, ref. Num "234"] (The new registry finger print is generated and

  stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security**

  value; [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and

  allowing processing to continue if the new registry security value is equal

to the stored registry security value.[Column 6, lines 32-36; column 10, lines

38-43] (The processing will not be allowed to continue if the new registry

security value is not equal with the stored security value. If this is the case, that

is if they are found to be different, then the comparison result will be reported.)

- **Generating a new user identity value associated with a user identity
and comparing the new user identity value to the stored user identity values** (As

explained above in Microsoft operating system, in the process of authentication,

generation of a user identity value or the hash value of the user password is inherently

included. For NT, user enters their password/could be a new password and the clients

hashes the user's new password, and generates the hash value or the user identity

value and encrypts the server's challenge with this hash and sends two responses to the

server: One response uses the LAN Manager hash and another response uses the

stronger NT hash. The server then compares the client's response hash with the client's

hash in the SAM Registry hive and this meets the limitation of generating a new user

identity value associated with a user identity and comparing the new user identity value

to the stored user identity values.)(For the source/explanation that the examiner used,

see reference U, page 2, second paragraph and since the limitation indicated at least

one choosen from the group consists of the above explanation is sufficient) and

**Obtaining an input responsive to a program attempting to access the

system registry, the input allowing processing to continue**. (Since the limitation

indicated at least one choosen from the group consists of the above explanation is

sufficient)

6.   <u>As per claims 3-4 and 12-13</u> **Kathrow** discloses a method as applied to claims 1 and

claim 10 above. Furthermore **Kathrow discloses the method wherein** generating a registry

security value associated with a system registry comprises: concatenating system registry information; and inserting the concatenated system registry information in a one-way function to obtain the registry security value. [Column 4, lines 26-column 5, line 25; figure 2, ref. Num "232"]

7. <u>As per claims 5-6 and 14-15</u> Kathrow discloses a method as applied to claims 1 and 10 above. Furthermore **Kathrow discloses the method wherein authenticating the system registry after reading the system registry comprises:**

- **Generating a new registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s]**; [Column 5, lines 41-62; figure 2, ref. Num "234"] (The new registry finger print is generated and stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security value**; [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and **allowing processing to continue if the new registry security value is equal to the stored registry security value.**[Column 6, lines 32-36; column 10, lines 38-43] (The processing will not be allowed to continue if the new registry security value is not equal with the stored security value. If this is the case, that is if they are found to be different, then the comparison result will be reported.)

8.   <u>As per claims 21-22</u> **Kathrow** discloses an apparatus as applied to claim 19 above. Furthermore **Kathrow discloses an apparatus** wherein the processor operable to receive instructions which, when executed by the processor, cause the processor to generate a registry security value associated with a system registry comprises the processor to concatenate system registry information; and to insert the concatenated system registry information in a function to obtain the registry security value. [Column 4, lines 26-column 5, line 25; figure 2, ref. Num "232"]

9.   **As per claims 23-24** . **Kathrow** discloses an apparatus as applied to claim 19

above. Furthermore **Kathrow discloses an apparatus** wherein the processor operable to

receive instructions which, when executed by the processor, cause the processor to

authenticate the system registry after reading the system registry comprises the process

:

- **Generating a new registry security value [Fingerprint of the registry file/s**
  which includes hash value of the Windows registry file/s]; [Column 5, lines
  41-62; figure 2, ref. Num "234"] (The new registry finger print is generated and
  stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security**
  value; [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and
  allowing processing to continue if the new registry security value is equal
  to the stored registry security value.[Column 6, lines 32-36; column 10, lines
  38-43] (The processing will not be allowed to continue if the new registry
  security value is not equal with the stored security value. If this is the case, that
  is if they are found to be different, then the comparison result will be reported.)

Claim Rejections - 35 USC § 102

10.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form

the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign
country or in public use or on sale in this country, more than one year prior to the date of
application for patent in the United States.

11.   **Claims 7-9, 16-18 and 25-27** are rejected under 35 U.S.C. 102(b) as being anticipated

by 9**Pereira**. (hereinafter referred as Pereira)(U.S. Patent No. 5, 809, 230)

12.   **As per claim 7-9, 16-18 and 25-27 Pereira** discloses a method

> **detecting an attempt to change a system registry;[column 4, lines 49-54;**
>
>> **column 4, lines 40-44; column 4, lines 49-51 column 10, lines 20-21]**
>
> **generating a user identity value associated with the user identity;[column 10,**
>
>> **lines 20-26]** (if the user enters the corresponding password user would be able
>>
>> to define/access resources in the registry)
>
> •   **Comparing the user identity value with a stored user identity value; (**In
>
> Microsoft operating system, in the process of authentication, generation of a user
>
> identity value or the hash value of the user password is inherently included. For NT,
>
> user enters their password and the clients hashes the user's password, and generates
>
> the hash value or the user identity value and encrypts the server's challenge with this
>
> hash and sends two responses to the server: One response uses the LAN Manager hash
>
> and another response uses the stronger NT hash. The server then compares the client's
>
> response hash with the client's hash in the SAM Registry hive.)(For the
>
> source/explanation that the examiner used, see reference U, page 2, second paragraph)
>
> and
>
> •   **Modifying the system registry in response to being provided the user**
>
>> **identity value equal to the stored user identity value.[column 10, lines 29-**
>
> **33]**(The access control program may use an application program interface (API) to
>
> modify the registry system file in accordance with the restricted list files generated by
>
> the access control program.)

Conclusion

13.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).
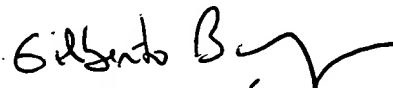
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S·L·

08/29/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100